SPOOFING

Information Security in Systems & Networks
Public Development Program

Sanjay Goel

University at Albany, SUNY

Fall 2006

Spoofing

Learning Objectives

- Students should be able to:
  - Determine relevance of spoofing attacks to specific business scenarios
  - Identify various types of spoofing
  - Recognize different spoofing attacks
  - Determine controls for spoofing

Spoofing

Basics

- Definition:
  - Computer on a network pretends to have identity of another computer, usually one with special access privileges, so as to obtain access to the other computers on the network
- Typical Behaviors:
  - Spoofing computer often doesn’t have access to user-level commands so attempts to use automation-level services, such as email or message handlers, are employed
- Vulnerabilities:
  - Automation services designed for network interoperability are especially vulnerable, especially those adhering to open standards.

Spoofing

Types

- **IP Spoofing:**
  - Typically involves sending packets with spoofed IP addresses to machines to fool the machine into processing the packets
- **Email Spoofing:**
  - Attacker sends messages masquerading as some one else
- **Web Spoofing:**
  - Assume the web identity and control traffic to and from the web server

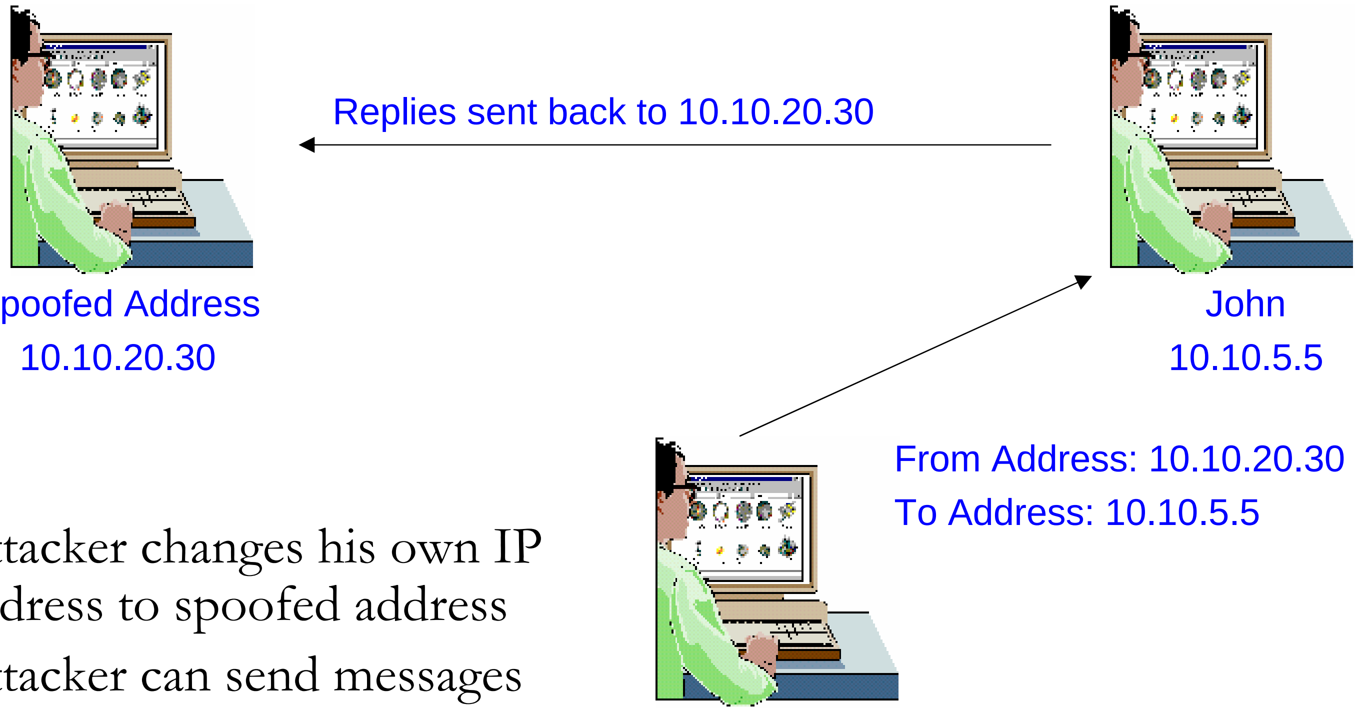
Spoofing

IP Spoofing: Definition

- Attacker uses IP address of another computer to acquire information or gain access to another computer
- Types
  - Basic Address Change
  - Use source routing to intercept packets
  - Exploit trust relationships on UNIX machines

Spoofing

IP Spoofing: Basic Address Change



Replies sent back to 10.10.20.30

Spoofed Address
10.10.20.30

John
10.10.5.5

From Address: 10.10.20.30
To Address: 10.10.5.5

Attacker
10.10.50.50

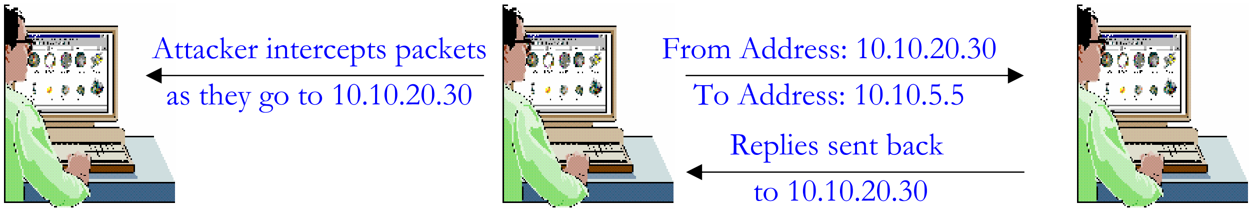
Steps

1. Attacker changes his own IP address to spoofed address
2. Attacker can send messages to a machine masquerading as spoofed machine
3. Attacker can not receive messages from that machine

Spoofing

IP Spoofing: Source Routing

- To facilitate two way traffic, attacker spoofs the address of another machine and inserts itself between the attacked machine and the spoofed machine to intercept replies
- The path a packet may change can vary over time so attacker uses source routing to ensure that the packets pass through certain nodes on the network



Attacker intercepts packets as they go to 10.10.20.30

From Address: 10.10.20.30
To Address: 10.10.5.5

Replies sent back to 10.10.20.30

Spoofed Address
10.10.20.30

Attacker
10.10.50.50

John
10.10.5.5

Spoofing

IP Spoofing: Prevention

- Prevention
  - Protect your machines from being used to launch a spoofing attack
  - Little can be done to prevent other people from spoofing your address
- Users can be prevented from having access to network configuration
- To protect your company from spoofing attack you can apply basic filters at your routers
  - Ingress Filtering: Prevent packets from outside coming in with address from inside.
  - Egress Filtering: Prevents packets not having an internal address from leaving the network

Spoofing

IP Spoofing: Unix Trust Relations

- In UNIX trust relationships can be set up between multiple machines
  - After trust becomes established user can use Unix r-commands to access sources on different machines
  - A .rhosts file is set up on individual machines or /etc/hosts.equiv is used to set it up at the system level
- Trust relationship is easy to spoof
  - If user realizes that a machine trusts the IP address 10.10.10.5 he can spoof that address and he is allowed access without password
  - The responses go back to the spoofed machine so this is a flying blind attack.
- Protection
  - Do not use trust relations
  - Do not allow trust relationships on the internet and limit them within the company
  - Monitor which machines and users can have trust without jeopardizing critical data or function

Spoofing

IP Spoofing: Prevention and Detection

- Prevention:
  - Limit system privileges of automation services to minimum necessary
  - Upgrade via security patches as they become available
- Detection:
  - Monitor transaction logs of automation services, scanning for unusual behaviors
  - If automating this process do so off-line to avoid "tunneling" attacks
- Countermeasures:
  - Disconnect automation services until patched
  - Monitor automation access points, such as network sockets, scanning for next spoof, in attempt to track perpetrator

Spoofing

Email Spoofing: Types

- Definition: Attacker sends messages masquerading as someone else. What are the repercussions?
- Types
  - Fake email accounts
  - Changing email configuration
  - Telnet to mail port

Spoofing

Email Spoofing: Basics

Reasons:

- Attackers want to hide their identity while sending messages (sending anonymous emails)
  - User sends email to anonymous e-mailer which sends emails to the intended recipient
- Attacker wants to impersonate someone
  - To get someone in trouble
- Social engineering
  - Get information by pretending to be someone else

Spoofing

Email Spoofing: Similar Name Account

- Create an account with similar email address
  - SanjayGoel@yahoo.com: A message from this account can perplex the students
  - Most mailers have an alias field (this can be used to prescribe any name.
- Example

Class:

I am too sick to come to the class tomorrow
so the class is cancelled. The assignments
that were due are now due next week.

Sanjay Goel

Spoofing

Email Spoofing: Similar Name Account

- Protection
  - Educating the employees in a corporation to be cautious
  - Make sure that the full email address rather than alias is displayed
  - Institute policy that all official communication be done using company email
  - Use PKI where digital signature of each employee is associated with the email

Spoofing

Email Spoofing: Modify Mail Client

- When email is sent from the user no authentication is performed on the from address
- Attacker can put in any return address he wants to in the mail he sends
- Protection
  - Education
  - Audit Logging
  - Looking at the full email address

Spoofing

Email Spoofing: Telnet to Port 25

- Telnet to port 25
  - Most mail servers use port 25 for SMTP.
  - An attacker runs a port scan and gets the IP address of machine with port 25 open
  - telnet IP address 25 (cmd to telnet to port 25)
  - Attacker logs on to this port and composes a message for the user.
- Example:

  Hello

  mail from:spoofed-email-address

  Rcpt to: person-sending-mail-to

  Data (message you want to send)

  Period sign at the end of the message

Spoofing

Email Spoofing: Telnet to Port 25

- Mail relaying is the sending of email to a person on a different domain
  - Used for sending anonymous email messages
- Protection
  - Make sure recipients’ domain same as mail server
  - New SMTP servers disallow mail relaying
  - From remote connection the from and to addresses are from same domain as mail server
  - Make sure spoofing and relay filters are configured

Spoofing

Web Spoofing: Types

- Web spoofing is the act of tricking a web browser into talking to a web server other than the intended server
  - Once spoofed the spoofed web server can send fake web pages or fool the victim into releasing personal information
  - It can be done by hacking the DNS that maps the server in a URL to a network address, or by modifying a Web page to have a bad URL, or by tricking your browser as it interprets CGI data, JavaScript, etc.
- Types
  - Registering a similar sounding domain
  - Man-in-the-Middle Attack
  - URL Rewriting
  - Tracking State

Spoofing

Web Spoofing: Registering new Domain

- No requirement against registering a domain
  - Attacker registers a web address matching an entity

    e.g. geproducts.com, gesucks.com
- Process
  - Hacker sets up site similar to authentic site
  - User goes to the spoofed site, orders items, and checks out
  - Site prompts user for credit card information
  - Gives the user a cookie
  - Puts message that site is experiencing technical difficulty
  - When user tries back spoofed site checks cookie
  - Directs the user back to legitimate site

Spoofing

Web Spoofing: Man in the Middle Attack

- **Man-in-the-Middle Attack**
  - Attacker inserts itself as a proxy between web server and client
  - Intercepts all communication and controls flow of information between client and server
  - Attacker has to compromise router or node through which the relevant traffic flows
- Protection
  - Secure perimeter to prevent compromise of routers

Web Spoofing

Web Spoofing: URL Rewriting

- **URL Rewriting**
  - Attacker redirects web traffic to another site that is controlled by the attacker
  - Attacker writes his own web site address before the legitimate link
  - e.g. <A href=“http://www.hacker.com/http://www.albany.edu/index.html”>
  - The user is first directed to the hacker site and then redirected to the actual site
- Protections
  - Web browsers should be configured to always show complete address
  - Ensure that code for website is properly protected at the server end and during transit

Spoofing

Web Spoofing: Tracking State

- Web Sites need to maintain persistent authentication so that user does not have to authenticate repeatedly
- Http is a stateless protocol
  - Tracking State is required to maintain persistent authentication
- This authentication can be stolen for masquerading as the user

Web Spoofing

Tracking State

- Three types of tracking methods are used:
  - Cookies: Text containing ID of the user stored in the cookie file
    - Attacker can read the ID from users cookie file
  - URL Session Tracking: An id is appended to all the links in the website web pages.
    - Attacker can guess or read this id and masquerade as user
  - Hidden Form Elements
    - ID is hidden in form elements which are not visible to user
    - Hacker can modify these to masquerade as another user

Spoofing

Web Spoofing: Protection

- Random hard to guess ID
  - Could be a random number in between 1 to 1000
- Use server side certificates
  - Certificates much harder to spoof
  - Users need to ensure that the certificates are legitimate before clicking on OK to accept certificate
- Protect the hard drive physically
  - Do not leave terminals unattended
- Use non-persistent cookies since hacker has to access and edit memory to get to it.
  - Keep session inactivity time low

Spoofing

Web Spoofing: Protection

- Disable JavaScript, ActiveX and other scripting languages that execute locally or in the browser
- Make sure that browser's URL address line is always visible
- User Education

Spoofing

Summary

- Spoofing is the false representation of a digital identity.
- Spoofing comes in three forms
  - IP Spoofing: using the IP address of another computer to gain access to unauthorized information.
  - Email Spoofing: masquerading as someone else through email.
  - Web Spoofing: having a web browser talk to a different web server than intended.
  - Various security controls are available to prevent and protect against spoofing.